| Sujet | Acronyme : **CoDeCQ** |
|---|---|
| | **Conception et décodage de codes correcteurs d'erreurs quantiques courts** |
| | |
| Direction de thèse | BUREL Gilles (Professeur) |
| Co-encadrement | SAOUTER Yannick (Chargé de Recherches CNRS) |
| | |
| Laboratoire | Lab-STICC – UMR CNRS 6285<br>(collaboration entre les équipes SI3 et CODES du Lab-STICC) |
| Etablissement | UBO |
| Période | Octobre 2023 à Septembre 2026 |
| | |
| Financement | ARED (Région Bretagne) 50 % et CDE (UBO) 50% |
| Contact | Yannick.Saouter@imt-atlantique.fr<br>Gilles.Burel@univ-brest.fr |

**Résumé du projet de thèse**

**Le projet vise à concevoir des codes quantiques courts et à améliorer les techniques de décodage associées dans le contexte des technologies quantiques : communication, cryptographie, calcul quantique. Dans le domaine de la conception, l'attention se portera sur les constructions à partir de codes classiques connus (codes Reed-Muller, BCH, …) ainsi que sur des constructions ad hoc de codes LDPC et turbo quantiques. D'un point de vue du décodage, une partie du travail consistera à adapter les techniques algébriques de décodage des codes classiques. Une autre partie portera sur l'amélioration des techniques de décodages itératives pour les codes LDPC et turbo.**

**Description de la thèse : - Sujet détaillé**

## Contexte d'étude :

Le domaine des **technologies quantiques** est un axe de recherche très actif comme en atteste l'implication de grandes entités comme IBM, Google et Intel, entre autres, au niveau mondial. Au niveau national, ATOS est un acteur majeur et les grands centres de recherches comme le CNRS, le CEA et l'INRIA se sont fortement positionnés sur le sujet et ont créé récemment des équipes de recherches internes dédiées à ce domaine. **Le but est d'initier la seconde révolution quantique** via l'ordinateur quantique, qui, grâce au parallélisme massif inhérent à la description des objets quantiques, laisse entrevoir un traitement rapide de calculs pour l'instant inaccessibles par les ordinateurs séquentiels classiques. **Cette percée affecterait un grand nombre d'activités industrielles** : les transports par l'optimisation des déplacements, la biologie pour le calcul des repliements de protéines par exemple, les semi-conducteurs par l'amélioration du placement et du routage des portes logiques, la programmation linéaire et toutes ses applications, etc … Des applications commerciales, comme la carte de crédit quantique sont aussi à l'étude. D'ores et déjà des applications réelles dans le domaine des **communications numériques inviolables** ont déjà été réalisées [1].

Un des problèmes rencontrés dans l'intégration de systèmes quantiques opérationnels, de tailles suffisantes est l'extrême sensibilité des objets quantiques au bruit ambiant ce qui peut mener à la décohérence des objets intriqués. Comme dans le cas des communications digitales classiques, une solution proposée [2] est l'emploi des **codes correcteurs**. Notre proposition de thèse se place dans cette optique et vise à élaborer des codes quantiques dédiés aux applications ainsi que de concevoir des procédures de décodage efficaces pour ce type de codes. Il s'agit d'ailleurs d'un des **axes d'action privilégié** par l'observatoire national de l'innovation scientifique et technique pour la sécurité dans le cadre des technologies quantiques [3].

Au niveau local, l'équipe SI3 du Lab-STICC, mène des recherches sur le sujet, en collaboration avec le LMBA (Laboratoire de Mathématiques de Bretagne Atlantique – UMR CNRS 6205), depuis 4 ans. Cela a donné lieu à 3 publications et deux thèses en cours (une thèse sur crédits établissement UBO, qui sera soutenue en 2023, et une thèse CIFRE avec Thalès, dans le cadre du GIS Cormorant, qui a démarrée en avril 2022). Les deux équipes SI3 et CODES peuvent aussi se prévaloir d'une longue expérience de 30 ans dans le domaine de la théorie de l'information classique et des codes correcteurs à décodage itératif comme les LDPCs et les turbocodes.

Le sujet de la thèse, les codes courts quantiques, se place dans la logique de l'extension du nombre de qubits dans les ordinateurs quantiques dans une optique d'une augmentation parcimonieuse de la complexité. Il est à noter aussi que les codes courts classiques sont également un sujet de recherche critique pour les applications des communications 5G et de l'internet des objets. Le développement des codes courts quantiques peut donc aussi bénéficier de manière transverse à ces thématiques et serait alors crucial pour les possibles applications de la technologie quantique à ces technologies.

**Contenu scientifique et objectifs :**

Un certain nombre de constructions pour des codes correcteurs quantiques ont déjà été suggérées. Les premières propositions utilisent des codes linéaires classiques (Reed-Muller, BCH, …) comme briques internes pour définir le code quantique. Plus récemment, des codes ad hoc à décodage itératif ont aussi vus le jour [4]. Chacune de ces deux approches amènent des problèmes spécifiques.

Dans le cas des codes formés à base de codes classiques, la technique de décodage la plus souvent employée est la méthode basée sur le calcul de syndrome. Cette méthode est efficace pour des codes correcteurs possédant un faible pouvoir de correction mais devient vite prohibitive quand la distance minimale du code augmente. Dans le cas des codes classiques, la solution généralement adoptée est de substituer le décodage algébrique utilisant les propriétés spécifiques du code à cette méthode. Dans le cas quantique et dans l'état actuel des recherches, l'attention a surtout été focalisée sur la construction des codes et non sur le décodage. Un premier travail au cours de cette thèse sera de rechercher des techniques pour transposer les techniques de décodage avancées (décodage majoritaire, Berlekamp-Massey, décodage par automorphisme …) à cette première famille de codes quantiques.

Le deuxième axe de recherche portera sur les codes à décodage itératif. Les recherches actuelles sur ce type de code s'intéressent peu à la notion de distance minimale du code. Or dans le cas classique, un certain nombre de travaux menés entre autres par les équipes SI3 et CODES du Lab-STICC, impliquées dans cette proposition de thèse, portaient explicitement sur la détermination et l'optimisation de cette valeur. Là encore, une partie du travail consistera à adapter ces techniques au cas quantique. Par ailleurs, certains de ces codes existent uniquement dans le cas quantique, comme les codes

topologiques. De nouvelles techniques pourraient s'avérer nécessaire pour ce type de code. Un deuxième point de la recherche portera sur les techniques de décodage. L'algorithme de référence est l'algorithme de propagation de croyance. Il peut donner des performances décevantes en particulier dans le cas des codes courts. Un certain nombre d'amélioration ont été récemment proposées comme la réponse linéaire ou le dépliement des cavités. Le travail portera donc sur l'élaboration d'algorithmes de substitution en prenant en compte le surplus de complexité. D'autres approches sont aussi envisageables comme le décodage par programmation linéaire ou les algorithmes utilisés en physique statistique comme la propagation d'espérance.

Pour conclure, on peut noter que la problématique de conception et de décodage de courts est aussi un sujet très étudié dans le cas des codes classiques dans une perspective d'applications à la **5G** ou à **l'internet des objets**. Les problématiques de ce domaine sont proches de celles des codes quantiques. Toute amélioration pourrait donc potentiellement bénéficier aux contextes classique et quantique. A plus long terme, on peut aussi imaginer une application des communications quantiques dans le domaine militaire pour développer des **transmissions sécurisées avec des drones**. En ce cas, les deux approches classiques et quantiques seraient complémentaires et directement applicables.

**Références**

[1] S-K Liao et al. *"*Satellite-to-ground quantum key distribution*". Nature 549 pp : 43-47, 2017.*
[2] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist,". Physical Reviews A, vol. 54, pp. 1098–1105, 1996.
[3] https://www.gendarmerie.interieur.gouv.fr/onists/ressources-documentaires/veille-technologique/calculateur-quantique-et-securite
[4] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons". Ann. Phys., vol. 303, p. 2, 2003.